EIGRP Best Practice

1) **Definire al massimo due o tre livelli architetturali**:

a) Core ed Aggregation;

b) Core, Aggregation and Access;

c) Definire le zone come topologia di rete (EIGRP non usa aree); una zona è definita come una failure domain dove link e devices failures all'interno di una zona debbono avere impatto minimo al di fuori della zona stessa.

d) Considerare le Choke Points quali elementi di interconnessione tra zone; provvedono a fornire informazioni di raggiungibilità e di topologia della rete e consente la configurazione di route summarization

e) in caso di architettura a due livelli:

CORE:

- applicare summarization routing verso il livello di aggregazione annunciando sole le best routes
- applicare politiche di controllo di routing (route policy) per stabilire quante e quali route accettare dal livello di aggregazione

AGGREGATION:

- provvede al collegamento del livello di accesso direttamente creando un profilo edge router;
- applica route summarization verso il livello di Core, mantenendo nascoste le IP subnets specifiche del livello di accesso verso il livello di Core;
- definire security policy a livello edge router usando tecniche di filtering layer 2 e layer 3 mantenendole il più vicino possibile alle sorgenti di traffico;

f) in caso di architettura a tre livelli:

CORE:

- applicare summarization routing verso il livello di aggregazione annunciando sole le best routes;
- applicare politiche di controllo di routing (route policy) per stabilire quante e quali route accettare dal livello di aggregazione;

AGGREGATION:

- applica route summarization sia verso il livello di Core che verso il livello di Accesso (attraverso i cosidetti Choke Points);
- non creare configurazioni di route summarization tra routers appartenenti allo stesso livello di aggregazione;
- implementare a questo livello le politiche di routing (route policy) per stabilire quante e quali route accettare dal livelli di accesso ed invece passare al livello di Core;
- performare traffic engineering (anche per evitare traffic black-holing e suboptima ìl routing in alcuni scenari), attraverso la redistribuzione diretta dal livelli del Core di routes più specifiche (non-summarized) oppure attraverso traffic filtering.

ACCESS:

- provvede al collegamento di IP prefix direttamente connesse via end-point
- Configurare il livello di accesso e quindi i router di tipo Spoke come Stub routers
- applicare a questo livello le security policy usando tecniche di filtering a livello 2 e layer 3

2) **Riduzione delle EIGRP query in caso di un fault o assenza di una route:**

a) non realizzare una soluzione alle query, attraverso multiple AS perché non risolve il problema di propagazione delle query con più AS e può aumentare l'eventualità di Stuck in Active (SIA) ossia quando un router non ha ancora ricevuto un reply alla query trasmessa entro un determinato periodo di tempo (circa 3 minuti)

b) Utilizzare invece le tecniche di Route Summarization e Stub, come pure route summarization e/o tecniche di filtering

c) Utilizza il livello di aggregazione per cercare di bloccare il propagarsi di query/reply, minimizzando al massimo le informazioni di routing tra il livello superiore Core ed il livello inferiore Access

3) **EIGRP Hub and Spoke:**

a) dai router Hub annunciare una default route verso i router Spoke;

b) considerare link point-to-point /31 tra routers Hun and Spoke;

c) In caso di dual-router Hub, considerare sempre le seguenti ed eventuali problematiche:

- route summarization black-holes: soluzione è collegare con un inter_hub link i due Hub router permettendo alla network " persa " di essere raggiunta attraverso il secondo hub e non droppata a causa della rotta summary in discard route configurata a garanzia di routing loops.

- route summarization suboptimal routing: soluzione è la configurazione chiamata leak-map applicata al router Hub dove la prefix più specifica (oltre alla summary route) da annunciare verso il router spoke è collegata (o direttamente connessa)

- Backdoor Link: si verifica quando esiste una connessione diretta tra due router Spoke: soluzione è la configurazione chiamata Stub Leaking che permette ai due router Spoke di annunciare un subset di routes imparate e garantire una ridondanza di raggiungibilità delle network in caso di fault

d) considerare i limiti di processor quando gli spoke sono collegati ai router Hub attraverso multiple interface

e) con una configurazione punto-multipunto attraverso una singola interface, verificare il limite di queue congestion (EIGRP ha una limitazione teorica di circa 400 peers per interface)

f) Configurare sempre i routers Spoke come Stub routers

g) Utilizzare BFD per la rilevazione di un failure di un nodo o link